National Aeronautics and Space Administration
Ames Research Center
Moffett Field, California 94035

X.509 CERTIFICATE POLICY

FOR

National Aeronautics and Space Administration (NASA)

Public Key Infrastructure (PKI)

December 17, 2004
Revision 1.3.1.2

National Aeronautics and Space Administration
Ames Research Center
Applied Information Technology Division
Moffett Field, CA. 94035-1000

X.509 Certificate Policy for NASA PKI

Signature:

____________________________ ________________

NASA Chief Information Officer Date

Table of Contents

1. Introduction

The National Aeronautics and Space Administration (NASA) operates a Public Key Infrastructure (PKI) to provide security for its electronic information. Programs that carry out or support NASA's missions may require the type of security services provided by a PKI. A PKI is a complex system that provides secure electronic data storage and exchange. Security is achieved by using public key cryptography. The types of security services provided by a PKI are:

- Confidentiality: The transformation of data into a form unreadable by anyone without the proper key
- Data Integrity: A service that addresses the unauthorized alteration of data by either confirming its integrity or warning about changes
- Authentication: The process whereby users or information sources prove that they are who they claim to be
- Non-repudiation: A service that limits denial of previous commitments or actions

These services are provided through public key cryptography's use of certificates and the public and private cryptographic keys associated with the certificates.

The primary function of a PKI is to manage these certificates and keys. A PKI manages the certificates through the following components:

- Certification Authority (CA): A trusted party that creates, renews, and revokes certificates.
- Registration Authority (RA): A trusted agent of the CA that verifies user identity.
- Certificate Repository*:* The public area in which users' public keys are stored. This is usually a directory such as X.500.
- Policy: The set of rules that guide the operation of the PKI.

The NASA PKI consists of a central NASA CA, RAs at each of the eleven NASA centers, and an X.500 directory for each NASA center. This document defines the Certificate Policy (CP) for the administration and operation of the NASA PKI. This document includes:

- Subscriber identification and authorization verification
- Control of PKI computer and cryptographic systems
- Operation of PKI computer and cryptographic systems, facilities and personnel
- Usage of keys and public-key certificates by Subscribers and Relying Parties
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met

This CP will be used by Certification Authorities (CAs) within the NASA PKI and by CAs outside the NASA PKI who wish to inter-operate with CAs within the NASA PKI. Please note definitions of terms used in this CP are provided in Appendix B. Terms defined in Appendix B are underlined the first time they appear in the CP.

Users of this document are to consult the Certification Practice Statement (CPS) of the Issuing NASA CA to obtain further details of the issuing NASA CA's implementation of this CP.

1.1 OVERVIEW

This CP follows and complies with the Internet Engineering Task Force (IETF) Request for Comment (RFC) 2527, X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

This CP defines the primary obligations and operational responsibilities of all NASA PKI program participants, and defines the creation, management and use of Version 3 X.509 public key certificates. Public key certificates are appropriate for use in applications requiring communication between networked computer-based systems and applications requiring electronic information integrity and confidentiality. Such applications include, but are not limited to, electronic mail, transmission of unclassified but sensitive information, digital signing of electronic forms, contract submission digital signatures, and authentication of infrastructure components such as web servers. Please note, the term, "X.509 certificates", as used in this CP implies X.509 Version 3 certificates. While this CP does not require the use of public key certificates in any particular NASA application or program, if public key certificates are used they must be used in accordance with this CP.

This CP supports medium level assurance, unless specified otherwise. As NASA adds other assurance levels, this CP will be modified to describe the policies for these levels. Please note that the term "assurance" refers to the level of trust associated with a certificate. The term, "assurance" is not intended to convey any representation or warranty as to 100% availability of a NASA CA's services offered under this CP. Such availability may be affected by system maintenance, system repair, or factors outside the control of a NASA CA.

Issuance of a public key certificate under any part of this CP

- is not to be used for protection of classified information
- does not imply that the Subscriber has any authority to conduct business transactions on behalf of the organization operating the NASA CA

The terms and provisions of this CP shall be interpreted under and governed by United States Federal law. The United States Government disclaims any liability that may arise from the use of this CP.

1.2 IDENTIFICATION

Upon identification by the NASA Policy Authority (PA), the applicable object identifiers (OIDs) will be included in NASA certificates. In the area of level of assurance, OIDs will be used to indicate the level of assurance associated with a certificate. A NASA CA will use the Federal Public Key Infrastructure four levels of assurance, rudimentary, basic, medium and high.

1.3 COMMUNITY & APPLICABILITY

This CP defines the policies under which the NASA PKI is administered and operated.

In compliance with NASA Procedures and Guidelines (NPG) 2800, Managing Information Technology section 2.2, as a policy within the jurisdiction of the NASA CIO, this CP applies to NASA organizations and NASA contractors and therefore NASA organizations and NASA contractors must comply with this CP, unless a waiver is obtained from the NASA CIO.

A NASA CA must adhere to this CP.

1.3.1 Certification Authority (CA)

A NASA CA operating under this CP is responsible for:

- the creation of End Entity Confidentiality (i.e. encryption) key pairs (if required)
- creation and signing of X.509 certificates binding Subscribers with their verification public key and encryption keys
- where permitted, creation and signing of X.509 certificates binding other CAs with their CA public keys
- promulgating certificate status through Certificate Revocation Lists (CRLs) and
- overview and enforcement of certificate policy within those entities

A cross-certification between a NASA CA and another CA shall be in accordance with this CP and any additional requirements determined by the NASA PA. All cross-certification will be done pursuant to instructions from the PA. Any agreements made with other CAs shall be documented and applicable disclaimers made available to Subscribers.

1.3.2 Registration Authorities (RAs)

A RA operating under this CP is responsible for End Entity administration on behalf of the NASA CA.

1.3.3 End Entities

1.3.3.1 Subscribers

A Subscriber may be an individual or an organization. A Subscriber is the entity whose name appears as the subject in a certificate. Subscribers may be issued certificates for assignment to devices, groups, organizational roles, or applications provided that responsibility and accountability is attributable to an individual or an organization.

NASA PKI certificates will only be issued after request or authorization for issuance from one or more NASA Sponsors. Certificates may be issued to NASA employees, NASA contractors, or organizations with which the Sponsor has relationships in conducting NASA business or research.

A NASA CA may administer any number of Subscribers.

1.3.3.2 Relying Parties

A Relying Party is an entity that relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party may be either a Subscriber of the NASA PKI or a Subscriber of a PKI that has signed a cross-certification agreement with the NASA PKI.

1.3.4 Applicability

Certificates issued under this CP shall only be used for transactions relating to NASA business. Certificates issued under this CP are suitable for providing confidentiality, electronic authentication, authorization and data integrity for NASA information up to and including Sensitive Unclassified.

The combination of this CP and associated certificates, can be used to protect NASA sensitive unclassified data including:

- mission information
- information that NASA is required by law or agreement to protect such as Privacy Act information and information provided to NASA by its contractors and subject to non-disclosure agreement
- proprietary business and technology information such as legal, payroll, personnel and contract proposal and source selection information
- electronic commerce transactions including EDI, e-mail, Web servers, SSL, etc.
- personnel information, including position, salary, benefits, health

1.3.5 Approved And Prohibited Applications

Applications for which issued certificates are suitable include the following:

- Applications that use or contain NASA sensitive unclassified information
- Electronic mail applications that use NASA standard electronic mail packages
- Web applications that contain NASA sensitive unclassified information
- Electronic forms used in conducting NASA business

Applications for which issued certificates are prohibited include the following:

- Applications that use or contain classified information
- Applications that have no relevance to NASA business

Approved and prohibited applications are identified by the NASA PA.

1.3.6 Repositories

A NASA CA shall ensure that there is at least one certificate and CRL repository associated with it. This repository should be in the form of one or more directories that comply with NASA X.500 standards.

Where the repository is not under the control of a NASA CA, the NASA CA shall ensure that the terms and conditions of its association with the repository include, but are not limited to, the subjects of availability, access control, and integrity of data.

1.4 CONTACT DETAILS

This CP is administered by the NASA Policy Authority, Office of the Chief Information Officer, Washington, D.C.

The contact person is:

Chairman, NASA Policy Authority
Office of the Chief Information Officer
National Aeronautics and Space Administration
Washington, DC 20546-0001

2. General Provisions

2.1 OBLIGATIONS

2.1.1 CA Obligations

A NASA CA will operate in accordance with its Certification Practice Statement (CPS), this CP, NASA policy, and U.S. Federal law and regulations when issuing and managing the keys provided under this CP. The NASA CA will ensure that all RAs operating on its behalf will comply with the relevant provisions of this CP concerning the operation of RAs. A NASA CA will take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, certificates, or End Entity hardware and software used in connection with the PKI.

A NASA CA must:

- publish a CPS
- have in place mechanisms and procedures to ensure that its RAs and Subscribers are aware of and agree to abide with the stipulations in this CP and the NASA CA's CPS to which it applies
- revoke the certificates of Subscribers found to have acted in a manner counter to those stipulations
- establish that any CA with whom it cross-certifies complies with all CPs that are mutually recognized
- through compliance audit, verify to cross-certifying CAs that it complies with this CP
- ensure that its certification services, issuance and revocation of certificates, and issuance of CRLs are in accordance with this CP

2.1.1.1 NOTIFICATION OF CERTIFICATE ISSUANCE AND REVOCATION

A NASA CA must make CRLs available to a Subscriber or Relying Party in accordance with section 4.4.

2.1.1.2 ACCURACY OF REPRESENTATIONS

When a NASA CA publishes a certificate, it certifies that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with this CP. Publication of the certificate in a public repository constitutes notice of such verification.

A NASA CA will provide to each Subscriber notice of the Subscriber's rights and obligations under this CP. Such notice will include a description of the allowed uses of certificates issued under this CP, the Subscriber's obligations concerning key protection, and procedures for communication between the Subscriber and the RA, including communication of changes in service delivery or changes to this CP. Such notice will also indicate procedures to address suspected key compromise, certificate or key renewal, service cancellation, and dispute resolution.

A NASA CA will ensure that any notice includes a description of a Relying Party's obligations with respect to use, verification, and validation of certificates.

2.1.1.3 TIME BETWEEN CERTIFICATE REQUEST AND ISSUANCE

No stipulation.

2.1.1.4 CERTIFICATE REVOCATION AND RENEWAL

A NASA CA will ensure that procedures for the expiration, revocation, and re-issuance of a certificate will conform to the relevant provisions of this CP and will be expressly stated in its CPS, the Subscriber Agreement, or any other applicable document outlining the terms and conditions of the certificate use. A NASA CA will also ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in sections 4.4.4 and 4.4.9. The address of the CRL must be defined in the certificate.

2.1.1.5 PROTECTION OF PRIVATE KEYS

A NASA CA shall ensure that its private keys and activation data are protected in accordance with sections 4 and 6.

A NASA CA shall ensure that the private keys that it holds or stores, and activation data are protected in accordance with sections 4 and 6.

A NASA CA shall ensure that any confidentiality (i.e. encryption) private keys of a Subscriber have been backed-up and are protected in accordance with section 6.

2.1.1.6 RESTRICTIONS ON ISSUING CA'S PRIVATE KEY USE

A NASA CA shall ensure that its certificate signing private key is used only to sign CA related activities such as signing certificates, CRLs and ARLs. A NASA CA may issue certificates to Subscribers, CA and RA personnel, devices and applications. A NASA CA may also issue cross-certificates to other CAs when expressly authorized by the NASA PA.

2.1.2 RA Obligations

A RA is obligated to conform to the stipulations of this CP and must comply with the NASA CA's CPS. A RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

An RA is responsible for bringing to the attention of Subscribers all relevant information pertaining to the rights and obligations of the NASA CA, RA, and Subscriber contained in this CP, the CPS, the Subscriber Agreement, if applicable, and any other relevant document outlining the terms and conditions of use.

A RA is accountable for transactions performed on behalf of the NASA CA.

2.1.2.1 NOTIFICATION OF CERTIFICATE ISSUANCE AND REVOCATION

A RA is obligated to conform to certificate issuance and revocation stipulations of this CP and to comply with the NASA CA's CPS.

There is no requirement for a RA to notify a Relying Party of the issuance or revocation of a certificate.

2.1.2.2 ACCURACY OF REPRESENTATIONS

When a RA submits Subscriber information to a NASA CA, it must certify to the NASA CA that it has authenticated the identity of that Subscriber in accordance with sections 3 and 4 and guidelines established in the NASA CA's CPS.

2.1.2.3 PROTECTION OF RA PRIVATE KEY

Each RA must ensure that his or her private keys are protected in accordance with sections 5 and 6.

2.1.2.4 RESTRICTIONS ON RA PRIVATE KEY USE

The RA will use the keys and certificates only for the purposes authorized by this CP and in conformance with a NASA CA's CPS.

2.1.3 Subscriber Obligations

The Subscriber is obliged to enter into an agreement or abide by an acceptable use policy which outlines the terms and conditions of use, including permitted applications and purposes.

2.1.3.1 ACCURACY OF REPRESENTATIONS

Any information required to be submitted to a NASA CA or RA in connection with a certificate must be complete and accurate.

2.1.3.2 PROTECTION OF SUBSCRIBER PRIVATE KEY AND KEY TOKEN

Subscribers are required to protect their private keys and key tokens (if applicable) in accordance with section 6, and to take all reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

2.1.3.3 RESTRICTIONS ON SUBSCRIBER PRIVATE KEY USE

The Subscriber will use the keys and certificates only for purposes related to NASA business and in conformance with this CP and a NASA CA's CPS.

2.1.3.4 NOTIFICATION UPON PRIVATE KEY COMPROMISE

Where a Subscriber suspects private key compromise, he or she must immediately notify the RA in a manner specified by this CP and in accordance with a NASA CA's CPS.

2.1.4 Relying Party Obligations

The rights and obligations of a Relying Party who is a member of this PKI are covered in this CP. The rights and obligations of a Relying Party belonging to another PKI must be addressed in the cross-certification agreement between the NASA PKI and the other PKI.

2.1.4.1 USE OF CERTIFICATES FOR APPROPRIATE PURPOSE

Relying parties must use the certificate only for the purposes for which it was issued and in accordance with this CP and a NASA CA's CPS.

2.1.4.2 VERIFICATION RESPONSIBILITIES

A Relying Party must use certificates only in accordance with the certification path validation procedure specified in the X.509 standard and IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

2.1.4.3 REVOCATION CHECK RESPONSIBILITY

Prior to using a certificate, a Relying Party must check the status of the certificate against the appropriate and current CRL in accordance with the requirements stated in section 4.4.9 of this CP. As part of this verification process, the digital signature of the CRL must also be validated.

2.1.5 Repository Obligations

Repositories that support a NASA CA in posting information as required in this CP shall maintain availability of CRLs in accordance with the requirements stated in section 4.4.9 of this CP. If applicable, repositories shall provide access control mechanisms sufficient to protect certificates and CRLs as provided in section 2.6.3 of this CP.

Repositories will be available on a schedule set forth by the NASA Chief Information Officer.

2.2 LIABILITY

NASA disclaims any liability that may arise from use of any certificate issued by or under the authority of NASA, or from the determination to revoke a certificate issued by or under the authority of NASA. In no event will NASA be liable for any damages, including, but not limited to, direct, indirect, special, consequential or punitive damages, arising out of or relating to any certificate issued or revoked by or under the authority of NASA.

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification By Relying Parties

No stipulation.

2.3.2 Fiduciary Relationships

Issuance of certificates by a NASA CA and assistance in that issuance by a NASA RA does not make NASA or its NASA CA or RA an agent, fiduciary, trustee, or other representative of requesters or relying parties, or others using the NASA PKI.

2.4 INTERPRETATION & ENFORCEMENT

2.4.1 Governing Law

United States Federal law shall govern the enforceability, construction, interpretation, and validity of this CP.

2.4.2 Severability, Survival, Merger, Notice

Severance or merger may result in changes to the scope, management, and/or operations of a NASA CA. In such an event, this CP may require modification as well. Should it be determined that one section of this CP is incorrect or invalid, the other sections shall remain in effect until the CP is updated. Requirements for updating this CP are described in section 8 of this CP. Responsibilities, requirements, and privileges of this CP are merged to the newer CP upon its release.

2.4.3 Dispute Resolution Procedures

Any dispute related to key and certificate management between NASA and an organization or individual outside of NASA shall be resolved using an appropriate dispute settlement mechanism. A dispute shall be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved through arbitration by the NASA PA.

A dispute related to key and certificate management within NASA shall be resolved by the Operation Authority for a NASA CA.

2.5 FEES

No stipulation.

2.6 PUBLICATION & REPOSITORY

2.6.1 Publication Of CA Information

A NASA CA will:

- publish a CPS on a web site maintained by, or on behalf of a NASA CA, the location of which must be identified in compliance with section 8 of this CP
- provide a full text version of the CPS when necessary for the purposes of any audit, accreditation, or cross-certification
- provide the following certificate information in the repository:

- all encryption public key certificates issued by a NASA CA to Subscribers
- all cross-certificates issued by a NASA CA to other CAs
- most recent CRL of public key certificates revoked by a NASA CA
- most recent Authority Revocation List (ARL) of cross-certificates revoked by a NASA CA

2.6.2 Frequency Of Publication

Certificates shall be published following Subscriber acceptance. CRL publication shall be in accordance with section 4 of this CP.

2.6.3 Access Controls

A NASA CA shall ensure, directly or through agreement with a repository, that repository access controls will be configured on certificates, certificate status information and CRLs and that only authorized personnel can write or modify the online version of this CP and a NASA CA's CPS.

Subscribers shall have read only access to this CP and a NASA CA's CPS.

2.6.4 Repositories

The NASA X.500 Directories will be used as the NASA certificate repository in order to facilitate the widest distribution of certificates.

2.7 COMPLIANCE AUDIT

A compliance audit determines whether a NASA CA's actual performance meets the standards established in its CPS and satisfies the requirements of this CP.

2.7.1 Frequency Of Compliance Audit

A compliance audit of a NASA CA will be performed annually.

The PA may order a compliance audit by an auditor at any time at its discretion.

A NASA CA shall reserve the right to require periodic and aperiodic inspections and audits of any RA facility within a NASA CA's domain to validate that the RA is operating in accordance with the security practices and procedures laid out in the NASA CA's CPS.

2.7.2 Identity/Qualifications Of CA Auditor

The PA will approve the auditor or auditing organization to be used for compliance audits. The auditor must perform CA or Information System Security Audits as its primary responsibility, demonstrate significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software.

2.7.3 Auditor's Relationship To Audited CA

The auditor performing the compliance audit can be contracted by NASA or can be an organization within NASA sufficiently separated from the audited NASA CA to provide an unbiased, independent evaluation.

2.7.4 Topics Covered By Audit

The purpose of the audit shall be to verify that the NASA CA is implementing its practices and policies in accordance with its CPS and this CP.

2.7.5 Actions Taken As A Result Of Audit

Any discrepancies between a NASA CA's operation, and the stipulations of its CPS shall be recorded by the auditor in a formal report to be submitted to the PA. In addition to noting any discrepancies, the auditor will note the severity of any discrepancies.

The PA in consultation with a NASA CA shall determine:

- the remedy for any noted discrepancies;
- a time for completing remedies to any discrepancies noted;
- if other parties require notification, in relation to the type and severity of any discrepancies. In the case of discrepancies classified as severe discrepancies, which affect other parties, the affected parties will be notified of the discrepancies and the actions being taken to remedy the discrepancies.

A remedy may include any of the following procedures:

- indicate the discrepancies, but allow the NASA CA to continue operations until the next programmed audit; or
- allow the NASA CA to continue operations for a maximum of thirty days pending correction of any problems prior to revocation; or
- suspend NASA CA operation

The decision regarding which of these actions to take shall be based on the severity of the discrepancies, the risks imposed, and the disruption to Subscribers.

2.7.6 Communication Of Results

Results of an audit shall be communicated to the NASA CA and to the PA, in accordance with this CP, and as defined by a NASA CA's CPS. Communication to Subscribers or other NASA personnel will depend on the discrepancies discovered and the remedies to be taken.

A NASA CA found not to be in compliance with its CPS or this CP shall be notified immediately at the completion of the audit. Required remedies shall be defined and communicated to the NASA CA as soon as possible to limit the risks created. The implementation of remedies shall be communicated to the PA. A special audit may be required to confirm the implementation and effectiveness of the remedy.

The method and detail of notification of audit results to CAs cross-certified with a NASA CA will be defined within the cross-certification agreement between the two parties. Unless specified in a particular cross-certification agreement, no communication of the audit results shall occur outside NASA.

2.8 CONFIDENTIALITY OF INFORMATION

All information that is not considered by the NASA PA to be public will be kept confidential. Specification of confidential information is addressed in the following subsections.

2.8.1 Types Of Information To Be Kept Confidential

The Subscriber's private signing key is confidential to that Subscriber. The NASA CA and RA are not provided any access to those keys.

The Subscriber's copy of his/her Confidentiality (i.e. encryption) private key must be kept confidential by the Subscriber. However, Confidentiality private keys may be backed-up by the issuing NASA CA or another party on behalf of the NASA CA, in which case these keys must be protected in accordance with section 6, and must not be disclosed to any other party without the prior consent of the Subscriber or Sponsor, unless required by law.

Personal or corporate information held by a NASA CA or RA, other than that which is explicitly published as part of a certificate, CRL, ARL, certificate policy, or this CP is considered confidential and shall not be released unless required by law.

Collection of personal information may be subject to collection, maintenance, retention and protection requirements of the Privacy Act of 1974, 5 U.S.C. 552a. Access to information stored locally by a NASA CA or RA shall be restricted to those with an official need-to-know in order to perform their official duties.

Information held in audit trails is considered confidential to NASA and shall not be released outside the agency, unless required by law.

Generally, the results of annual audits are kept confidential, with exceptions as outlined in section 2.7.

Any keys held by a NASA CA shall be released only to an organizational authority, in accordance with a NASA CA's CPS and this CP, or a law enforcement official, in accordance with US law and this CP (see section 2.8.4).

2.8.2 Types Of Information Not Considered Confidential

Information included in public certificates, CRLs, and ARLs issued by a NASA CA are not considered confidential.

Information in this CP is not considered confidential.

Confidentiality of relevant information in the directory is achieved through the use of access controls.

2.8.3 Disclosure Of Certificate Revocation Information

When a certificate is revoked/suspended, a reason code is included in the CRL entry for the action. This reason code is not considered confidential. However, no other details concerning the revocation are normally disclosed.

2.8.4 Information Release

A NASA CA will not disclose certificate or certificate-related information to any third party, except when:

- authorized by this CP or the NASA CA's CPS.
- required to be disclosed by law, U.S. governmental rule or regulation, or court order.
- required to release information to law enforcement officials, consistent with the NASA agency policy.
- authorized by the Subscriber when necessary to effect an appropriate use of the certificate. A NASA CA may choose to further define or restrict the Subscriber's authority to disclose certificate or certificate-related information.

Any requests for the disclosure of information must be signed and delivered to the NASA CA.

2.8.5 Release As Part Of Civil Discovery

To release information as part of civil discovery, the NASA CA will comply with the NASA agency policy.

2.8.6 Other Information Release Circumstances

No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

The U.S. Government, as represented by the Administrator of the National Aeronautics and Space Administration, retains exclusive right to any product or information developed by NASA under or pursuant to this CP including, but not limited to, any public key certificates and private keys that it issues. The rights to any product or information developed by a U.S. Government contractor under or pursuant to this CP will be governed by the terms of the contract and U.S. federal laws and regulations. Rights in the NASA name, initials, Seal and other devices are governed by section 311 of the National Aeronautics and Space Act of 1958, as amended (42 U.S.C. 2459b) and regulations at 14 CFR Part 1221.

3. Identification & Authentication

3.1 Initial Registration

3.1.1 Types Of Names

Names for certificate issuers and certificate subjects are of the X.500 Distinguished Name (DN) form. The National Aeronautics and Space Administration is a registered name in accordance with ANSI, the US National Name Registration Authority. A single naming hierarchy is established within NASA as outlined below:

- Names for certificate issuers (i.e. a NASA CA) and certificate subjects (i.e. Subscriber or End Entity) are of the X.500 Distinguished Name (DN) form. These names are unique and unambiguous within the NASA hierarchy as specified in the NASA Directory Service Architecture, Standards and Products document.
- Certificate issuers shall have entries at the organizationName level. The DNs will follow the following form: cn=CA name, o=National Aeronautics and Space Administration, c=US.
- Certificate subjects shall have entries at the organizationalUnitName level. The DNs will follow the following form: cn=Jane Doe, ou=NASA Center name, o=National Aeronautics and Space Administration,c=US.

All attributes identified in this section are as defined in ITU-T Recommendation X.521 *Information Technology – Open Systems Interconnection – The Directory: Selected Object Classes* (1988).

Certificate subjects may choose an optional Alternated Subject Name in which case this object should be marked non-critical. Certificate subjects may choose to have additional name forms, such as an email address, however the DN is the primary name and the one used to populate the subject fields of certificates, CRLs, and ARLs.

Additional objects outside the scope of this CP shall also be present in the naming hierarchy.

3.1.2 Need For Names To Be Meaningful

The contents of each certificate Subject and Issuer name field must have an association with the authenticated name of the Entity.

A certificate issued for a device or application must include within the Directory entry the name of the person or organization responsible for that device or application.

3.1.3 Rules For Interpreting Various Name Forms

As the NASA Center responsible for management and operation of the NASA X.500, Marshall Space Flight Center is responsible for the NASA X.500 directory name space.

3.1.4 Uniqueness Of Names

Distinguished names must be unique for all End Entities of a NASA CA. X.500 distinguished names shall be used, and a NASA CA and RAs shall enforce name uniqueness within the X.500 name space, which they have been authorized.

3.1.5 Name Claim Dispute Resolution Procedure

No stipulation

3.1.6 Recognition, Authentication And Roles Of Trademarks

A NASA CA may establish cross-certification with other CA domains outside the NASA PKI. The naming and trademark issues associated with those names within those domains is outside the scope of this CP.

3.1.7 Method To Prove Possession Of Private Key

Prior to the issuance of a certificate, the Issuing NASA CA and End Entity will confirm their respective identities through the use of a shared secret. The proof-of-possession approaches described in the IETF RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols are suitable for this requirement.

Prior to the exchange of a private decryption key the Issuing NASA CA and End Entity will confirm their respective identities through the use of a shared secret. The proof-of-possession approaches described in the IETF RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols are suitable for this requirement.

3.1.8 Authentication Of Organization Identity

Public key certificates shall be issued to individuals whenever possible. For those cases in which there are several individuals acting in one capacity, a certificate may be issued that contains the name of an organization.

An application for an organization to be a Subscriber must be made by an individual authorized to act on behalf of the prospective Subscriber (i.e. organization). This authorized individual must be the person in the organization who will be responsible for ensuring control of the certificate and the associated private keys, including accounting for which individual of the organization has control of the keys at what time. In addition, in the case of an organization, the confidentiality (i.e. encryption) key pair shall be used but the digital signature key pair shall not be used.

Identification and authentication of the prospective Subscriber must be by the following means:

- requests for organizational certificates shall include the organization name, address, and documentation of the existence of the organization.
- the RA or NASA CA must examine notarized copies of documentation providing evidence of the existence of the organization.
- the RA or NASA CA must also verify the identity and authority of the individual acting on behalf of the prospective Subscriber and their authority to receive the keys on behalf of that organization.

- the RA or NASA CA must keep a record of the type and details of identification used.
- the RA or NASA CA must retain the name of the person to whom the organizational certificate is issued.

The procedures for issuing an organizational certificate shall not conflict with other stipulations of this CP(e.g., key generation, private key protection, and user obligations).

In the case of issuing cross-certificates to other CAs, the NASA CA may issue cross-certificates to the CAs of contractors and partners. The NASA PA will review the policies and procedures of the other CA before approving a cross-certification.

The NASA PA will authenticate the other CA using existing business agreements between NASA and the other CA's organization or through searches of recognized databases of registered corporations, or by presentation of the organization's articles of incorporation to the NASA PA. In all cases, the authentication documentation shall be filed and retained by the NASA PA.

3.1.9 Authentication Of Individual Identity

An application for an individual to be a Subscriber must be made by the individual. In addition to the identification and authentication described below, the prospective Subscriber must personally present him or herself to the RA for authentication prior to certificate issuance.

It is the responsibility of a RA to verify the identity of the Subscriber applying for a certificate. A RA must obtain confirmation of the Subscriber's identity and affiliation with NASA. A RA must file and retain authentication documentation described below.

Confirmation of the individual's affiliation with NASA must be through one of the following means:

- For most NASA personnel proof of affiliation is provided through the identification badge issued to the individual at his/her entrance-on-duty. For the badge to be considered confirmation of affiliation, the badge issuer must have received official notification of the individual's affiliation.
    - ➢ *For civil servants*, the badge issuer must receive notification of employment from the Center's Human Resources department. The badge issuer must retain this notification. Examples of acceptable notification include official federal employment forms or written and signed notification from a Center's Human Resources hiring officials.
    - ➢ *For contractors*, the badge issuer must receive confirmation from the contractor's Contracting Officer's Technical Representative (COTR) or Technical Monitor.

- For NASA Centers in which the badge process does not meet the requirement noted above, a RA must receive and retain notification of the individual's affiliation. For civil servants, a RA must first receive written and signed confirmation from the Center's Human Resources department. For contractors, a RA must first receive written and signed confirmation from the contractor's COTR or Technical Monitor.

Confirmation of the individual's identity must be through one of the following means:

- For some NASA Centers, identity checks may be performed as part of the initial hiring and badge procedure for civil servants and/or contractors. If so, a RA must retain a copy of the form used to collect and verify the identity information (ex. NASA form 531) or show access to a database or file where the information is retained.

- If a NASA Center does not provide identity checks, a RA must perform the identity verification or be shown a form of identification for which an identity check has previously been performed.
  - For RAs performing identity verification, the RA must record and retain the information checked along with the sources used to check the information.
  - For a RA accepting other forms of identification, the identification provided must include a picture. An RA accepting a form of identification must make a copy of the form of identification accepted or record and retain the following:
    - ✓ the form of identification accepted
    - ✓ any unique identification information associated with the form, such as passport number or driver's license number
    - ✓ any expiration information associated with the form

3.1.10 Authentication Of Devices Or Applications

A device or application can be named as certificate subjects. In such cases, the device or application must have a human sponsor. Application must be made by an individual or organization to which the device or application is attributable. Identification and authentication of the applicant must follow section 3.1.8 or 3.1.9 as if that individual or organization was applying for the certificate on its own behalf.

A RA must also verify the identity of the individual or organization making the application and their authority to receive the keys for that device or application.

A RA must keep a record, file, and retain the type and details of identification used.

3.2 AUTHENTICATION FOR ROUTINE REKEY

The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a relying party. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key, a different serial number, and may be assigned a different validity period.

A request for re-key may only be made by the Entity in whose name the keys have been issued. Only Entities that are NASA civil servants may request re-key on the basis of existing Subscriber certificates. All other Entities must identify themselves as in an initial request, in accordance with section 3.1.

For cross-certification relationships, no automatic rekey will be provided. If the NASA PA determines that a cross-certification agreement is to extend beyond the original period, a new cross-certificate is issued, prior to expiration of the current one. The same identification and authentication process used for initial cross-certification agreements applies to the issuance of new keys.

3.3 AUTHENTICATION FOR REKEY AFTER REVOCATION

For Subscribers whose certificates have been revoked, rekey will not be permitted until the identification and authentication requirements for initial registration are repeated, except in the following situations:

- an organizational change within NASA results in changes to the Distinguished Names of several employees
- a Subscriber is temporarily unable to present himself or herself in person (e.g. on extended travel) and the revocation was not due to a key compromise

For revoked cross-certificates, no rekey will be done until the identification and authentication requirements are repeated.

3.4 AUTHENTICATION OF REVOCATION REQUEST

A NASA CA or RA acting on its behalf must authenticate a request for revocation of a certificate. A NASA CA must set out in its CPS the process by which it addresses such requests and the means by which it will establish the validity of the request. A NASA CA's revocation process must be in accordance with section 4.4 of this CP.

Requests for revocation of a certificate must be logged.

4. Operational Requirements

4.1 APPLICATION FOR A CERTIFICATE

A NASA CA must ensure that all procedures and requirements with respect to an application for a certificate are set out in its CPS and are in compliance with this CP.

The following steps will be required in the certificate application process:

- applicant will submit a written certificate request, signed and dated by the appropriate authorities (as defined in the NASA CA's CPS),
- RA or CA will establish the identity of the certificate requester per sections 3.1.8 and 3.1.9, and
- applicant will sign an agreement or an acknowledgement of the applicable terms and conditions governing their use of the certificate

An application for a certificate does not oblige a NASA CA to issue a certificate.

4.2 CERTIFICATE ISSUANCE

Upon completion of the certificate application process per section 4.1, a NASA CA will:

- build and sign a certificate, with confirmation from its RAs
- publish the certificate in the NASA repository
- send the certificate to the Subscriber

The issuance and publication of a certificate by a NASA CA indicates a complete and final approval of the certificate application.

For information on delivery of key pairs for certificate issuance, please refer to sections 6.1.2 and 6.1.4 of this CP.

4.3 CERTIFICATE ACCEPTANCE

Acceptance is the action by a Subscriber that triggers the Subscriber's duties and potential liability. A NASA CA will ensure, in its CPS, a technical or procedural mechanism to

- explain to the Subscriber its responsibilities as defined in section 2.1.3
- require the Subscriber to indicate acceptance of the responsibilities and the certificate for medium assurance, the Subscriber will sign a document or statement noting that they have read and accepted these responsibilities.

The ordering of this process, and the mechanisms used, will depend on factors such as where key s are generated and how certificates are posted.

For a device or application, the individual or organization that is responsible for the device or application may do acceptance.

4.4 CERTIFICATE SUSPENSION & REVOCATION

4.4.1 Circumstances for revocation

A certificate must be revoked when the certificate is no longer trusted. Reasons for certificate revocation are:

- the Subscriber's employment is terminated or Subscriber is suspended for cause
- private keys are compromised or suspected of compromise
- when identifying information or attributes in the certificate changes before the certificate expires (i.e. organizational change)
- media holding the private key is compromised or suspected of compromise
- failure of the Subscriber to meet the Subscriber obligations under this CP, the NASA CA's CPS, any agreement, or any applicable law
- the Subscriber or other authorized party (as defined in section 4.4.2) requests that the certificate be revoked

A cross-certificate issued by a NASA CA to an external CA shall be revoked when the certificate is no longer trusted for any reason or if the relationship is no longer required. Reasons for cross-certificate revocation are:

- compromise or suspected compromise of private keys
- corporate mergers or take-overs
- failure of the cross-certified CA to meet their obligations as stated in the cross-certification agreement
- unexpected changes to the business relationship between the two entities

4.4.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- the Subscriber in whose name the certificate has been issued
- the individual or organization who made the application for the certificate on behalf of a device or application
- the Subscriber's management, if the Subscriber is a NASA employee or contractor
- personnel of the Issuing NASA CA
- personnel of an RA associated with the Issuing NASA CA
- a NASA Center's Information Technology (IT) Security Manager
- the NASA PA

4.4.3 Procedure For Revocation Request

A NASA CA must ensure that all procedures and requirements with respect to the revocation of a certificate are described in its CPS. Requests for revocation must provide identification of the certificate to be revoked, an explanation of the reason for revocation, and allowances for the request to be authenticated (e.g., digitally or manually signed). In addition, the requester shall appear in person before the NASA CA or RA processing the revocation request. Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties.

Upon receipt and confirmation of the revocation request, the NASA CA or RA shall revoke the certificate and shall record the event. A confirmed revocation request, and any resulting actions taken by the NASA CA or RA, must be retained. When a certificate is revoked, a detailed description of the reason for the revocation must also be documented.

When a Subscriber's certificate is revoked, the revocation will be published in the appropriate CRL. Revoked certificates shall remain on the CRL until the certificate expires. When a cross-certificate is revoked the revocation will be published in the ARL of the Issuing NASA CA.

4.4.4 Revocation Request Grace Period

Action in response to a request for revocation must be initiated within twenty-four (24) hours of receipt. A NASA CA's revocation request grace period may be shorter than 24 hours; if there are circumstances under which a NASA CA needs to take immediate action, these shall be spelled out in its CPS.

4.4.5 Circumstances For Suspension

A NASA CA may disable/suspend a Subscriber's certificate if a Subscriber goes on leave. A NASA CA may disable/suspend a Subscriber's certificate in support of a security investigation by internal NASA security personnel or external law enforcement agencies. Unlike revocation, disabling a Subscriber allows for re-enabling at a later time.

Information on public keys of disabled Subscribers is not available in the NASA repository, but it is retained in a NASA CA database. Once the certificate is disabled/suspended, the Subscriber's keys are not available for encryption or signing. However, any files that were signed, prior to the suspension, may be verified by recipients.

Cross-certificates will not be suspended.

4.4.6 Who Can Request Suspension

The parties identified in section 4.4.2 can also request disabling/suspending a certificate.

4.4.7 Procedure For Suspension Request

A NASA CA must ensure that all procedures and requirements with respect to the suspension of a certificate are set out in its CPS. Requests for suspension must provide identification of the certificate to be suspended, an explanation of the reason for suspension, and allowances for the request to be authenticated (e.g., digitally or manually signed).

Upon receipt and confirmation of the suspension request, the NASA CA or RA shall suspend the certificate and shall record the event. A confirmed suspension request, and any resulting actions taken by the NASA CA or RA, must be retained.

4.4.8 Limits On Suspension Period

The requesting party shall stipulate limits.

4.4.9 CRL Issuance Frequency

A NASA CA must ensure that it issues an up to date CRL at least every twelve hours, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required; if there are circumstances under which a NASA CA will post early updates, these shall be spelled out in its CPS.

A NASA CA must also ensure that its CRL issuance is synchronized with any directory synchronization to ensure the accessibility of the most recent CRL to Relying Parties. A NASA CA shall ensure that superseded CRLs are removed from the directory system upon posting of the latest CRL.

4.4.10 CRL Checking Requirements

A Relying Party must check the status of all certificates in the certificate validation chain against the current CRLs and ARLs prior to their use. A Relying Party must also verify the authenticity and integrity of CRLs and ARLs.

If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this CP.

4.4.11 On-line Revocation/Status Checking Availability

The NASA PKI does not currently support on-line revocation/status checking.

4.4.12 On-line Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms Of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements For Other Forms Of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Related To Key Compromise

For information on key compromise, please refer to section 4.8.3. of this CP.

4.5 SYSTEM SECURITY AUDIT PROCEDURES

4.5.1 Types Of Events Recorded

A NASA CA shall record in audit log files all events relating to the security of a NASA CA system. These include:

NASA CA System [application software] Events

Audit log changes

- any changes to audit log parameters such as audit frequency, types of events audited
- attempts to modify or delete the audit logs

Authentication

- successful and unsuccessful attempts to login and authenticate as a CA trusted role
- changes in rules for authentication
- maximum number of unsuccessful authentication attempts during login
- if applicable, changes in the type of authentication (e.g. changing from password to biometrics)

Key Generation

- CA key generation actions including CA key changeover (not mandatory for single session or one-time use symmetric keys)

Private Key Access

- access to private keys retained within a NASA CA for key recovery purposes
- export of private keys (keys used for single session are excluded)

Public Key Entry, and Deletion

- changes to public keys (including additions and deletions)

Certificate Management Requests and Actions

- all certificate management requests and subsequent actions to include:
  - certificate registration or creation
  - certificate changes to include:
    - ➢ update
    - ➢ suspension/disable
    - ➢ recovery
  - certificate revocation

Certificate Revocation List Management Actions

- all certificate revocation list actions

Directory Posting Actions

- posting of CA and certificate information to a directory

Account and Policy Administration

- addition or deletion of roles and entities

- changes to access privileges of roles or entities
- changes to a NASA CA's policies as implemented within a NASA CA's software

NASA CA System and Application Administration Events

- system start-up and shutdown
- logon to a NASA's CA application software
- re-set or change to passwords
- back-up or restore of a NASA CA's application database
- access to a NASA CA's application database
- installation, removing or destruction of hardware cryptographic module
- as applicable, file manipulation (e.g. creation, renaming, moving)
- software check integrity failures
- resetting operating system clock
- changes to a NASA CA server configuration to include hardware, software, operating system and patches

NASA CA Facility Access Events

- access to room housing a NASA CA to include notification of violations to physical access security

NASA CA Support Systems Events

- Uniterruptible Power Supply (UPS) failure

Other events

Tokens (if applicable)

- loading certificates to tokens
- zeroing of tokens

All logs, whether electronic or manual, should contain the date and time of the event along with the identity of the entity which caused the event. In addition, for some types it will be appropriate to record the success or failure, the source and destination of a message, or the disposition of a created object (e.g., a filename).

A NASA CA must ensure that the CPS indicates what information is logged.

4.5.2 Frequency Of Audit Log Processing

A NASA CA must ensure that its audit logs are reviewed at least once every two weeks. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Supporting logs from the NASA CA and RA should be compared when any action is deemed suspicious.

A NASA CA must identify the audit log processing frequency in its CPS.

4.5.3 Retention Period For Audit Log

A NASA CA must keep its audit logs onsite for at least two months and subsequently retain them in the manner described in section 4.6 of this CP.

4.5.4 Protection Of Audit Log

An electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion.

A NASA CA must specify procedures for the protection of audit log(s) in its CPS. A NASA CA shall identify a responsible party to perform audit log reviews. This responsible party performing an audit log review shall not be allowed to modify an audit log.

4.5.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed up. A NASA CA must specify in its CPS procedures for the backup of audit log(s) and procedures for off-site storage of audit logs to occur on a monthly basis.

4.5.6 Audit Collection System

A NASA CA must identify and specify the operation of an audit collection system in its CPS.

4.5.7 Notification To Event Causing Subject

Where an event is logged by the audit collection system, notification to the individual, organization, device, or application that caused the event is neither required nor prohibited in this CP.

A NASA CA must identify its approach to notification to event causing subject(s) in its CPS.

4.5.8 Vulnerability Assessments

A NASA CA, CA System Administrator and other operating personnel shall be watchful for attempts to violate the integrity of the certificate management system. A NASA CA shall use the processes identified in section 4.5 of this CP to monitor, assess, and address system vulnerabilities as required.

4.6 RECORDS RETENTION

4.6.1 Types Of Data Retained

At a minimum the following data shall be retained:

- certificates issued (private signing keys are not backed up)
- audit information as identified in section 4.5
- certificate requests/approvals includes certificate issuance, revocation, suspension and recovery
- identification and authentication information submitted by Subscribers
- CRLs and ARLs issued
- CA Certification Practice Statement

- CA system and equipment configuration and modifications to CA system and configuration
- documentation required for compliance audits
- record of CA re-key
- if applicable, documentation of receipt of tokens
- If applicable, CA accreditation
- If applicable, contractual agreements

4.6.2 Period For Record Retention

Information identified in section 4.6.1 shall be preserved, maintained, and disposed of in accordance with NASA Records Retention and Schedules, NPG 1441.

4.6.3 Protection Of Record Retention

Record retention material must be protected either by physical security alone, or a combination of physical and cryptographic protection. Any record retention site must provide adequate protection from environmental threats such as temperature, humidity, and magnetism.

A NASA CA must identify the record retention protection in its CPS.

4.6.4 Records Retention Backup Procedures

No stipulation

4.6.5 Requirements For Time-Stamping Of Records

No stipulation.

4.6.6 Records Retention Collection System

A NASA CA must identify the records retention collection system in its CPS, to include the packaging and transmittal of retained data.

4.6.7 Procedures To Obtain And Verify Retained Information

Only authorized personnel should be allowed access to retained information. The contents of the record retention shall not be released except as determined by the PA and in accordance with the NASA Records Retention and Schedules. A NASA CA must identify the procedures to obtain and verify retained information in its CPS.

4.7 KEY CHANGEOVER

NASA employees shall receive automatic key update. As such, both the encryption and digital signature key pairs are automatically updated prior to expiration. All other Subscribers shall apply to renew his or her key pair.

The CA signing key may be changed. Once the signing key is changed the new key will be used for signing and the old key can be used to verify the old signature until the lifetime of the old signing key expires.

A NASA CA must identify the details of the key changeover process in its CPS.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing Resources, Software, And/Or Data Are Corrupted

A NASA CA must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software, and/or data. In the case of business continuity, a NASA CA operation shall be re-established as quickly as possible with priority given to the ability to generate certificate status information.

When a repository is not under the control of the NASA CA, a NASA CA must ensure that all agreements with the repository provide that business continuity procedures be established and documented by the repository.

A NASA CA must identify the compromise process in its CPS.

4.8.2 Entity Key Recovery

A NASA CA must provide key recovery capability. The NASA CA must identify its key recovery process(es) in its CPS.

4.8.3 Entity Key Compromise

In the event of compromise or suspected compromise of a NASA CA signing key, the NASA CA must immediately notify the PA and all CAs to whom it has issued cross-certificates.

In any key compromise situation, the Entity must notify the Issuing NASA CA or its RA immediately.

A NASA CA must ensure that its CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.8.4 Disaster Recovery

A NASA CA must establish a disaster recovery plan, which outlines the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. When a repository is not under the control of a NASA CA, a NASA CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

A NASA CA must identify the disaster recovery process in its CPS.

4.9 CA TERMINATION

All issues relating to a NASA CA termination must be presented to the PA for oversight of the termination process. In the event of termination, a NASA CA in cooperation with the PA must notify its Subscribers, notify all CA's with whom it is cross-certified, revoke all certificates it issued, and arrange for the continued retention of the NASA CA's keys and information.

The NASA CA records retention should be retained in the manner and for the time period indicated in section 4.6 of this CP.

5. Physical, Procedural & Personnel Security

5.1 Physical Controls

5.1.1 Site Location And Construction

A NASA CA site must:

- satisfy at least the requirements for a High-Security Zone (please refer to Appendix B for the definition of a High-Security Zone)
- be a locked facility to which only authorized personnel have access
- be manually or electronically monitored for unauthorized intrusion at all times
- ensure access to the CA server is limited to those personnel identified on an access list
- ensure personnel not on the access list are properly escorted and supervised
- ensure a site access log is maintained and audited periodically

5.1.2 Physical Access

A NASA CA physical access requirements are included in section 5.1.1.

If a RA is permitted to submit on-line requests to the NASA CA, the RA site must provide appropriate security protection of the cryptographic module and a RA's private key. RA equipment shall be protected from unauthorized access while activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the equipment is not activated.

Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). Private keys stored on a hard drive must be secured through cryptographic mechanisms. For added security the Subscriber may physically secure the hard drive using access control software/hardware, or the Subscriber may store their private keys on a removable diskette and store media in a locked drawer when the media is not being used.

5.1.3 Power And Air Conditioning

The facility that houses a NASA CA's equipment shall be supplied with power and air conditioning sufficient to create a reliable operating environment.. The actual quantity and quality of utility service will depend on how the facility operates, e.g., its times of operation (24 hours/7 days or 8 hours/5 days).

A NASA CA's equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

This CP makes no stipulation on prevention of exposure of a NASA CA's equipment to water beyond that called for by best business practice. A NASA CA's equipment shall be installed such that it is not in danger of exposure to water.

5.1.5 Fire Prevention And Protection

This CP makes no stipulation on prevention of exposure of a NASA CA's equipment to fire beyond that called for by best business practice. An automatic fire extinguishing system shall be installed in accordance with local policy and code.

5.1.6 Media Storage

A NASA CA must ensure that storage media used by a CA system are protected from environmental threats such as temperature, humidity, and magnetism.

5.1.7 Waste Disposal

Media used for the storage of information such as keys, activation data, or CA files is to be sanitized or destroyed before released for disposal.

Normal office waste shall be removed or destroyed in accordance with local policy.

5.1.8 Off-site Backup

A NASA CA shall have an off-site back-up. A NASA CA must ensure that facilities used for an off-site backup CA have the same level of security and controls as the primary CA site and as stipulated in this CP.

In the area of system backup, a NASA CA shall perform a full system back-up sufficient to recover from system failure for off-site storage on at least a monthly basis.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust for a PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

The trusted roles for the NASA PKI are defined in the following sections.

5.2.1.1 CA TRUSTED ROLES

The NASA CA's role and the corresponding procedures a NASA CA will follow shall be defined in detail in its CPS. However, a NASA CA must provide the following basic criteria:

- a NASA CA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection. Each person's system access is to be limited to those actions for which they are required to perform in fulfilling their responsibilities.
- a NASA CA should provide for a minimum of three distinct PKI personnel roles, distinguishing between day-to-day operation of the CA system, the management and audit of those operations and the management of substantial changes to requirements on the system including its policies, procedures or personnel**.** An example of a division of responsibilities between the three roles is provided below:

  Master User
  - ➢ configuration and maintenance of the CA system hardware and software

  Officer
  - ➢ management of Administrators and other Officers
  - ➢ commencement and cessation of CA services
  - ➢ verification of audit logs
  - ➢ oversight of CA system audit log retention

  Administrator (or RA)
  - ➢ management of the Subscriber initialization process
  - ➢ creation, renewal or revocation of certificates
  - ➢ distribution of tokens (where applicable)

An alternative division of responsibilities is permitted so long as it provides the same degree of resistance to insider attack**.**

5.2.1.2 RA TRUSTED ROLES

A RA's role and the corresponding procedures a RA will follow shall be defined in detail in a NASA CA's CPS. Primarily, a RA's responsibilities are:

- acceptance of subscription, certificate change, certificate revocation/suspension and key recovery requests
- verification of an applicant's identity
- transmission of applicant information to the NASA CA
- receiving and distributing authorization codes for on-line key exchange and certificate creation

5.2.2 Number Of Persons Required Per Task

A separate individual shall be identified for each trusted role. A NASA CA must identify in its CPS those operations that are sensitive and require multiple authorizations. To perform sensitive operations a minimum of two individuals shall be required. These individuals should use a split knowledge technique such as twin passwords to perform any sensitive operation. An example of a sensitive operation is one that involves access to a Subscriber's private keys stored by the NASA CA, such as key recovery.

5.2.3 Identification & Authentication For Each Role

Identification and authentication for NASA CA personnel shall follow requirements identified In sections 5.3, 5.3.1, and 5.3.2. The items in these sections must be performed before NASA CA personnel are:

- included in the access list for the CA site
- included in the access list for physical access to the CA system
- given a certificate and account on the CA system for the performance of their role. Each of these certificates and accounts (with the exception of CA signing certificates) must:
  - be directly attributable to an individual
  - not be shared
  - be restricted to actions authorized for that role through the use of CA software, operating system, and procedural controls.

5.3 PERSONNEL SECURITY CONTROLS

Personnel performing duties with respect to the operation of a NASA CA or RA must:

- be appointed by an approving authority
- have received comprehensive training with respect to the duties they are to perform
- not be assigned duties that may cause a conflict of interest with their NASA CA or RA duties

A NASA CA shall identify in its CPS, the individual or group responsible for the operation of a NASA CA.

5.3.1 Background, Qualifications, Experience, And Clearance Requirements

NASA CA and RA roles are deemed to be positions of “Public Trust” per the Office of Personnel Management (OPM) 5 CFR Parts 731, 732, and 736. Personnel filling these roles shall successfully complete investigations for Public Trust positions.

5.3.2 Background Check Procedures

All background checks must be performed in accordance with NASA Personnel Security Policies.

5.3.3 Training Requirements

Personnel performing duties with respect to the operation of a NASA CA or RA must receive training in:

- the CA/RA security principles, mechanisms, and stipulations of this CP and the NASA CA’s CPS
- the operation of the software and/or hardware used in the CA system
- the duties they are expected to perform

A NASA CA’s personnel will receive orientation in a NASA CA’s business resumption or disaster recovery plan procedures.

5.3.4 Retraining Frequency And Requirements

The requirements of section 5.3.3 must be kept current to accommodate changes in the CA system. Refresher training shall be conducted in accordance with these changes.

5.3.5 Job Rotation

No stipulation.

5.3.6 Sanctions For Unauthorized Actions

Any CA or RA personnel that operates in violation of the policies and procedures stated herein may have their access to the CA system revoked and may be subject to administrative discipline and possible criminal prosecution.

Repeated or significant violations of this CP by the CA or RA organization may result in revocation of the CAs or RAs public key certificate.

5.3.7 Contracting Personnel

Contractor personnel employed to operate any part of a NASA CA or RA shall be subject to the same criteria as a US Government employee and shall be cleared to the position specified in section 5.3.1.

5.3.8 Documentation Supplied To Personnel

A NASA CA must make available to its CA and RA personnel the certificate policies it supports, its CPS, and documentation sufficient to define duties and procedures relevant to their position.

6. Technical Security Controls

6.1 Key Pair Generation And Installation

6.1.1 Key Pair Generation

A digital signature key pair must be generated by the Subscriber using a Federal Information Processing Standard (FIPS) approved algorithm.

A confidentiality (i.e. encryption) key pair must be generated using a Federal Information Processing Standard (FIPS) approved algorithm.

Digital signature and encryption key pairs must be generated using FIPS 140 validated cryptographic module(s).

The methods of key pair generation shall be stipulated in a NASA CA's CPS.

6.1.2 Private Key Delivery To Entity

In most cases, private keys will be generated and remain within the cryptographic boundary of the cryptographic module. If the Subscriber generates the key, then there is no need to deliver the private key. If the private key is not generated by the Subscriber, then it must be delivered to the Subscriber in an on-line transaction in a secure manner.

The methods used for private key delivery shall be stipulated in a NASA CA's CPS.

6.1.3 Public Key Delivery To Certificate Issuer

The digital signature public key must be delivered to a NASA CA either via an on-line transaction in accordance with the IETF RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols, or via an equally secure manner.

If the public encryption key is not generated by a NASA CA, then it must be delivered to a NASA CA in an on-line transaction in a secure manner.

The methods used for public key delivery shall be stipulated in a NASA CA's CPS.

6.1.4 CA Public Key Delivery To Users

A NASA CA public key must be delivered to the Subscriber in an online transaction in a secure manner.

The methods used for NASA CA public key delivery shall be stipulated in a NASA CA's CPS.

6.1.5 Asymmetric Key Sizes

Key pairs for Entities must be either 1024 bit RSA or DSA with Secure Hash Algorithm version 1 (SHA-1) or better.

The asymmetric key sizes used by a CA for Entity key pairs shall be stipulated in a NASA CA's CPS.

The asymmetric key sizes used by a CA for signing shall be stipulated in a NASA CA's CPS.

6.1.6 Public Key Parameters Generation

A NASA CA that utilizes the DSA must generate parameters in accordance with FIPS 186-2.

6.1.7 Parameter Quality Checking

Parameters for DSA shall be checked as specified in FIPS 186-2.

6.1.8 Hardware/software Key Generation

NASA CA digital signature key pairs must be generated in a hardware cryptographic module. Key pairs for all other Entities may be generated in a software or hardware cryptographic module. Software key generation process shall comply with FIPS 140-1 level 1. Hardware used in key generation/storage shall be compliant with higher level 2 and above of FIPS validation.

6.1.9 Key Usage Purposes (as per X.509v3 field)

Digital signature key pairs may be used for authentication, non-repudiation and message integrity. Encryption key pairs may be used for session key establishment. CA signing key pair are the only keys permitted to be used for signing certificates, CRLs and ARLs

6.2 PRIVATE KEY PROTECTION

The Subscriber must protect their private keys from disclosure. Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). Private keys stored on a hard drive must be secured through cryptographic mechanisms. For added security the Subscriber may physically secure the hard drive using access control software/hardware, or the Subscriber may store their private keys on a removable diskette and store media in a locked drawer when the media is not being used.

A NASA CA may allow subscribers to export their public and private keys using Public Key Cryptography Standards (PKCS)#12 export. In this case, the stipulations for private key protection noted in section 6.2 apply to all exportations of the private key and the storage mechanisms/locations of the exported private key. The NASA CA shall stipulate methods used for PKCS#12 export in a NASA CA's CPS.

The CA private keys must be protected by a combination of cryptographic software and hardware mechanisms. The level of protection must be adequate to deter a motivated attacker with substantial resources.

6.2.1 Standards For Cryptographic Module

The relevant standard for cryptographic modules is FIPS 140-1. The PA may determine that other comparable validation, certification, or verification standards are sufficient. The PA will publish these standards.

Section 6.8 provides more information on cryptographic modules.

The cryptographic module standards used by a NASA CA shall be stipulated in a NASA CA's CPS.

6.2.2 Private Key Multi-person Control

Multiple person control must be required for private key recovery. Two staff members performing duties associated with the roles of Officer or Administrator must participate or be present.

A NASA CA may allow subscribers to recover their own keys. In this case the two person participation will be replaced with a secure method that is consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63. A NASA CA shall stipulate the methods for Subscriber self key recovery in a NASA CA's CPS.

6.2.3 Private Key Escrow

Under no circumstances shall a signature key be escrowed.

6.2.4 Private Key Backup

A NASA CA must back up confidentiality (i.e. encryption) private keys. The Entity may also make a backup of the key. Backed-up keys must be stored in encrypted form.

An Entity may optionally back up its own Digital Signature private key. If so, the keys must be copied and stored in encrypted form.

A NASA CA shall back up the CA signature key to create a copy of the signature key that may be kept at the CA location; a second copy may be kept at the CA backup location.

The methods used for CA signature key backup shall be stipulated in a NASA CA's CPS.

6.2.5 Private Key Retention

Private signature keys supporting non-repudiation services shall never be backed up.

Section 4.6 provides more information on key retention.

6.2.6 Private Key Entry Into Cryptographic Module

Private keys are to be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

6.2.7 Method Of Activating Private Key

The Entity must be authenticated to the cryptographic module before the activation of the private key. This authentication may be in the form of a password, passphrases or PINs. Entry of activation data must be protected from disclosure (e.g., the data should not be displayed while it is entered).

In cases where a NASA CA has allowed subscriber's to export their keys, the stipulations for private key activation in section 6.2.7 apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

6.2.8 Method Of Deactivating Private Key

Cryptographic modules that have been activated must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g. via a manual logout procedure, or by a passive timeout. Hardware cryptographic modules should be removed and stored when not in use.

When keys are deactivated they must be cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be overwritten before the space is released to the operating system.

When deactivated, private keys must be kept in encrypted form only.

In cases where a NASA CA has allowed subscriber's to export their keys, the stipulations for private key deactivation in section 6.2.8 apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

6.2.9 Method Of Destroying Private Key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed. For software cryptographic modules, this may be overwriting the data. For hardware tokens, this may be executing a “zeroize” command. Physical destruction of hardware should not be required. The PA must approve the method of destruction.

In cases where a NASA CA has allowed subscriber's to export their keys, the stipulation for destroying the private key for software cryptographic modules in section 6.2.9 applies to all exportations of the private key and the storage mechanisms/locations of the exported private key.

Private key destruction procedures must be described in a NASA CA’s CPS.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Retention

The public key is retained as part of the certificate retention.

6.3.2 Usage Periods For The Public And Private Keys

Suggested validity period 1024 bit keys:
NASA CA public key and certificate - 20 years
NASA CA signing key – 20 years
End Entity public key and certificate - two years
End Entity private key (i.e. signing key)- 70% of public key certificate

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation And Installation

Any activation data must be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where passwords are used, an Entity must have the capability to change their password at any time. Passwords shall be generated in conformance with the NASA Procedures and Guidelines (NPG) 2810.1 Security of Information Technology, section A.6.3.1. [NPG 2810.1, section A6.3.1 provide equivalent guidelines to the guidelines in FIPS 112 Password Usage].

In cases where a NASA CA has allowed subscriber's to export their keys, the stipulations for activation data in section 6.4.1 apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

If data used for Entity initialization must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Activation data should be memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

In the process of entering activation data for login, a facility shall be included that provides for temporary application termination or account lockout after a predetermined number of login attempts.

Activation data shall never be shared.

In cases where a NASA CA has allowed subscriber's to export their keys, the stipulations for activation data protection in section 6.4.2 apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

6.4.3 Other Aspects Of Activation Data

This CP makes no stipulation on the life of activation data; however, if passwords are used the usage periods should be in accordance with NPG 2810.1.

In cases where a NASA CA has allowed subscriber's to export their keys, the stipulations for passwords as activation data in section 6.4.3 apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

The activation data used by a NASA CA shall be stipulated in a NASA CA's CPS.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

A NASA CA server must include the following functionality:

- access control to CA services and PKI roles
- enforced separation of duties for PKI roles
- identification and authentication of PKI roles and associated identities
- use of cryptography for session communication and database security
- retention of CA and End Entity history and audit data
- audit of security related events
- recovery mechanisms for keys and the CA system

This functionality may be provided by the operating system, or through a combination of operating system, CA software and physical safeguards.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

This CP makes no stipulation concerning the design and development of CA software other than CA software designed specifically for NASA shall follow NASA recognized development methodology such as SEL-81-305, Recommended Approach to Software Development.

6.6.2 Security Management Controls

The life-cycle security controls shall follow the guidelines specified in the NPG 2810.1 Security of Information Technology.

For NASA CA security management:

- a CA shall have a mechanism and/or policies in place to control and monitor the CA system configuration.
- the CA equipment shall be dedicated to administering a key management infrastructure.

- the CA equipment shall not have installed applications or component software, which are not part of the CA configuration with the exception of security software such as virus protection.
- the CA equipment updates shall be installed by trusted and trained personnel in a defined manner.

6.7 Network Security Controls

A NASA CA server must be protected from attack through any open or general purpose network with which it is connected. Remote access to a NASA CA system is secured using a secure communications protocol. No other remote access is permitted and features including inbound FTP are disabled. All TCP/IP ports shall be blocked, except those required by a CA enabled event auditing and the audit of all failed operations and low-frequency successes.

6.8 Cryptographic Module Engineering Controls

All NASA CA Digital Signature key generation, NASA CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 3.

The RA Administrator Digital Signature key generation and signing operations must be performed to at least a cryptographic module rated to at least FIPS 140-1 Level 1. As Level 2 hardware is made available across NASA, Digital Signature key generation and signing operations should be performed using Level 2 hardware

All other NASA CA and RA cryptographic operations must be performed with cryptographic modules validated to at least FIPS 140-1 Level 1.

End Entities must use cryptographic modules validated to at least FIPS 140-1 Level 1.

7. Certificate & CRL Profiles

7.1 CERTIFICATE PROFILE

7.1.1 Version Number

This CP supports X.509 Version 3 certificates.

A NASA CA must issue X.509 Version 3 certificates, in accordance with the X.509 standard and IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

The base (non-extension) X.509 fields supported:

Signature:	CA signature to authenticate certificate
Issuer:	name of CA
Validity:	activation and expiry date for certificate
Subject:	Subscriber’s distinguished name
SubjectPublicKeyInformation:	algorithmID, key
Version:	version of X.509 certificate, version 3 (2)
SerialNumber:	unique serial number for certificate

7.1.2 Certificate Extensions

A NASA CA must identify in its CPS the use of any extensions supported by the NASA CA, its RAs and End Entities.

7.1.3 Algorithm Object IDs

The NASA CA must use and End Entities must support FIPS approved algorithms for signing, verification, and symmetric key encryption.

7.1.4 Name Forms

In general, the name form used will be the Distinguished Name. In a certificate, the issuer DN and subject DN fields contain the full X.500 Distinguished Name of the certificate issuer or certificate subject.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Upon identification by the NASA PA, certificates issued under this CP shall assert the Policy OID appropriate to the level of assurance specified in the CP.

7.1.7 Usage Of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax And Semantics

No stipulation.

7.1.9 Processing Semantics For The Critical Certificate Policy

No stipulation.

7.2 CRL PROFILE

7.2.1 Version Number

A NASA CA must issue X.509 version 2 CRLs in accordance with the IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

7.2.2 CRL And CRL Entry Extensions

A NASA CA must identify in its CPS the use of any extensions supported by the NASA CA, its RAs and End Entities.

8. Specification Administration

8.1 SPECIFICATION CHANGE PROCEDURES

This CP will be reviewed in its entirety every year by the NASA PA. Errors, updates, or suggested changes to this document shall be communicated to the contact in section 1.4.

8.1.1 Items That Can Change Without Notification

Changes to items within this CP which, in the judgement of the PA, will have no or minimal impact on the Subscribers and cross-certified CA domains using certificates and CRLs issued under this CP, may be made with no change to the document version number and no notification.

8.1.2 Changes With Notification

Changes to the certificate policies supported by this CP as well as changes to items within this CP which, in the judgement of the PA may have significant impact on Subscribers and cross-certified CA domains using certificates and CRLs issued under this CP, may be made with 30 days notice and the version number of this document must be increased accordingly.

8.1.2.1 LIST OF ITEMS

Any items in this CP may be subject to the notification requirement as identified in sections 8.1.1 and 8.1.2.

8.1.2.2 NOTIFICATION MECHANISM

Thirty days prior to major changes to this CP, notification of the upcoming changes will be posted on a NASA web site and conveyed to cross-certified CA organizations via secure email. The notification shall contain a statement of proposed changes; the final date for receipt of comments; and the proposed effective date of change. The PA may request NASA CAs to notify their Subscribers of the proposed changes.

8.1.2.3 COMMENT PERIOD

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

8.1.2.4 MECHANISM TO HANDLE COMMENTS

Comments on proposed changes must be directed to the PA. Such communication must include a description of the change, a change justification, contact information for the person requesting the change, and signature of the person requesting the change.

The PA shall accept, accept with modifications, or reject the proposed change after completion of the comment period. Decisions with respect to the proposed changes are at the sole discretion of the PA.

8.1.2.5 PERIOD FOR FINAL CHANGE NOTICE

The PA will determine the period for final change notice.

8.1.2.6 ITEMS WHOSE CHANGE REQUIRES A NEW POLICY

If a policy change is determined by the PA to warrant the issuance of a new policy, the PA may assign a new Object Identifier (OID) for the modified policy.

8.2 PUBLICATION & NOTIFICATION PROCEDURES

The PA will publish this CP on a NASA web site. This CP is published at URL. http://nasaca.nasa.gov/. The PA will also disseminate information via email to any inquiries.

A NASA CA must make its CPS available to its Subscriber and Relying Parties at a NASA CA's World Wide Web site.

8.3 CPS APPROVAL PROCEDURES

The PA will make the determination that a NASA CA's CPS complies with this CP. The NASA CA must have, and meet all requirements of, an approved CPS prior to commencing operations.

Appendix A: Acronyms

ARL	Authority Revocation List
CA	Certification Authority
COTR	Contracting Officer’s Technical Representative
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DES	Data Encryption Standard
DN	Distinguished Name
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
EDI	Electronic Data Interface
FIPS PUB	(US) Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
NASA	National Aeronautical and Space Administration
NPG	NASA Procedures and Guidelines
NIST	National Institute of Standards and Technology
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PA	Policy Authority
RA	Registration Authority
RFC	(IETF) Request For Comments
RSA	Rivest-Shimar-Adleman
SHA-1	Secure Hash Algorithm
SP	Special Publication
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol

Appendix B: Definitions

Activation Data

Private data, other than keys, that are required to access cryptographic modules.

Assurance

How well a Relying Party can be certain of or trust the certificate.

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Level of assurance depends on multiple factors that include the proper registration of Subscribers, the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of the CP. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates

Authority Revocation List (ARL)

A list of revoked CA certificates. An ARL is a CRL for CA cross certificates.

Basic Level of Assurance

This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

CA Signing Key

The private portion of the CA signing key pair which is used to digitally sign certificates, certificate revocation lists and authority revocation lists.

CA Signing Key Pair

The key pair used by the CA for digitally signing. It consists of the CA signing (private) key and the CA public(verification) key

CA Public Key

The public key portion of the CA signing key pair which is used to verify certificates, certificate revocation lists and authority revocation lists signed by the CA signing key.

Certificate

The public key of a user, together with some other information, rendered unforgeable by digitally signing it with the private key of the certification authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

Certification Policy (CP) A document that defines the policies of a Certificate Authority (CA). A CP addresses all aspects associated with generation, production, distribution, recovery and administration of digital certificates. A CP also defines the policies for administration and operation of a CA.

Certification Practice Statement (CPS) A statement of practices that a CA employs to implement the specific policies defined in the Certification Policy (CP).

Certificate Revocation List (CRL) A list of revoked certificates that is created and signed by the same CA that issued the certificates. A certificate is added to the list if it is revoked (e.g., because of suspected key compromise). In some circumstances the CA may choose to split a CRL into a series of smaller CRLs.

Certification Authority An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

Cross-certification The process of establishing a trust relationship between two Certification Authorities. A process by which two Certification Authorities (CAs) securely exchange keying information so that each can certify the trustworthiness of the other's keys. Once the CAs has cross-certified, users within the CA domains can validate each other's certificates.

Digital Signature The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:
(a) whether the transformation was created using the key that corresponds to the signer's key; and
(b) whether the message has been altered since the transformation was made.

Directory A directory system that conforms to the ITU-T X.500 series of Recommendations.

Employee An employee is any person employed by NASA.

End Entity An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End Entity may be a Subscriber, a Relying Party, a device, or an application.

Entity Any autonomous element within the Public Key Infrastructure. This may be a CA, a RA or an End Entity.

High Level of Assurance
This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

High-security Zone
An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors. High-Security Zones should be separated by a perimeter. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.

Issuing CA
In the context of a particular certificate, the issuing CA is the CA that signed and issued the certificate.

Key
In cryptography, a secret value that is used in an encryption algorithm to encrypt and decrypt data.

Key Pair
Two mathematically related keys having the following properties:
1.) one key can be used to encrypt a message that can only be decrypted using the other key
2.) knowing one key, it is computationally infeasible to discover the other key.

MD5
One of the message digest algorithms developed by RSA Data Security Inc.

Medium Level of Assurance
This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.

Object Identifier
(OID) The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. OIDs are used by Certification Authorities to provide information to interfacing applications on policies the CA supports.

Organization
A department, agency, corporation, partnership, trust, joint venture or other association.

Operation Authority
Personnel who are responsible for the overall operation of a NASA CA. Their responsibility covers areas such as staffing, finances, and dispute resolution. The Operation Authority role does not require an account on the CA workstation.

Public Key

The portion of the public key pair that is available to everyone. The public key is stored in the directory. The NASA PKI uses a public key for encryption and a public (i.e. verification) key for verifying a digital signature.

Public Key Cryptography

Public key cryptography is a cryptographic system that uses key pairs. One key of the pair is public and the other key is private and known only to the owner. The mathematical relationship between the keys is such that an action performed by one key (i.e. encryption) can be undone by the other key (i.e. decryption). In addition, the relationship between the keys is such that knowing the public key does not compromise the private key. The NASA PKI uses two key pairs, one pair for encryption and one pair for signing.

Public Key Cryptography Standards

The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. PKCS documents have become widely referenced and implemented.

Public Key Cryptography Standards #12

This standard specifies a portable format for storing or transporting a user's private keys, certificates, miscellaneous secrets, etc.

Public Key Infrastructure

A structure of hardware, software, people, processes and policies that uses Digital Signature technology to provide Relying Parties with a verifiable association between the public component of an asymmetric key pair with a specific Subscriber.

Policy Authority

A NASA body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the NASA PKI.

Private Key

The portion of the public key pair that is kept secret by the owner of the key pair. The NASA PKI uses a private key for encryption and a private signing key for digital signatures.

Reason Code

A code put in the certificate to indicate the reason why the certificate was revoked.

Registration Authority (RA)

An Entity that is responsible for the identification and authentication of certificate Subscribers before certificate issuance, but does not actually sign the certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party

A person who uses a certificate signed by a NASA CA to authenticate a digital signature or to encrypt communications to the certificate subject, and is a Subscriber of a NASA CA or a PKI which is cross certified with the NASA PKI.

Rudimentary Level of Assurance

This level provides the lowest degree of assurance concerning identity of the individual. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality.

Sensitive Unclassified

Information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes.

Sponsor

A Sponsor in the NASA PKI is the NASA department or civil servant that has nominated that a specific individual or organization be issued a certificate. (E.g., for an employee this may be the employee’s manager). The Sponsor is responsible for informing the CA or RA if the relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

Subscriber

An individual or organization whose public key is certified in a public key certificate. In the NASA PKI this could be a civil servant, or a NASA contractor. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates - one containing their Digital Signature key; the other containing their Confidentiality (i.e. encryption) key.

Verification Public Key

The public key portion of a signing key pair used to verify data that has been signed by the corresponding signing private key.

REFERENCES

The documents noted below were referenced in the CP.

FIPS 112 Password Usage, May 1985.

FIPS 140-1 Security Requirements for Cryptographic Modules, January 1994.

FIPS 186-2 Digital Signature Standard (DSS), January 2000.

NPG 1441 NASA Records Retention and Schedules

NPG 2800 Managing Information Technology, September 1998.

NPG 2810.1 Security of Information Technology, August 1999.

PRIVACT 5 U.S.C. 552a, The Privacy Act of 1974.

RFC 2459 X.509 Public Key Infrastructure Certificate and CRL Profile, Housley, Ford, Polk and Solo, January 1999.

RFC 2510 X.509 Public Key Infrastructure Certificate Management Protocols , Adams and Farrell, March 1999.

RFC 2527 X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Chokhani and Ford, March 1999.

SEL-81-305 Recommended Approach to Software Development, r3, June 1992.

X.521 Information Technology-Open Systems Interconnection-The Directory: Selected Object Classes, 1988.

U.S.C. 2459b, The National Aeronautics and Space Act, as amended.